

BURSOR & FISHER, P.A.

L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

Counsel for Plaintiffs

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

M.D., O.F., and J.P., individually and on behalf
of all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC and META PLATFORMS,
INC.,

Defendants.

Case No. 3:24-cv-06369-AMO

**FIRST AMENDED CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

Plaintiffs M.D., O.F, and J.P. (collectively, “Plaintiffs”) bring this class action complaint on behalf of themselves and all others similarly situated (the “Class Members”) against Defendants Google LLC (“Google”) and Meta Platforms, Inc. (“Facebook”)¹ (together with Google, “Defendants”). Plaintiffs bring this action based on personal knowledge of the facts pertaining to themselves, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. This is a class action brought on behalf of all patients who accessed and used www.bluechew.com (the “Website”) to purchase prescription medication.

2. Dermacare, LLC d/b/a BlueChew (hereinafter, “BlueChew”) provides “a technology platform which enables registered users to connect with physicians and other health care providers for the diagnosis and treatment of erectile dysfunction.”² The Website offers patients convenient and discrete access to prescription medications for the treatment of this medical condition.

3. Information concerning an individual’s healthcare and prescription medication is protected by state and federal law. Despite these protections, and unbeknownst to Plaintiffs and Class Members, this sensitive, personal information communicated through the Website was intercepted by some of the largest advertising and social media companies in the country, including Facebook and Google.

4. Defendants intercepted this protected information through tracking technology embedded on the Website, including software development kits (“SDK”) and tracking pixels.

5. The protected information intercepted by Defendants was not aggregated or deidentified nor were Defendants prohibited from using this information for their own benefit. Defendants intentionally targeted and used this information for their own purposes, including for targeted advertising.

6. Plaintiffs and Class Members provided their personal information, including

¹ In October 2021, Facebook, Inc. changed its name to Meta Platforms, Inc. Unless otherwise indicated, Facebook, Inc. and Meta Platforms, Inc. are referenced collectively as “Facebook.”

² BlueChew, Terms and Conditions, <https://bluechew.com/terms-and-conditions>.

1 prescription information, to BlueChew with the expectation that this information would remain
2 confidential and private. Defendants' interception of this information without explicit consent
3 constitutes an extreme invasion of Plaintiffs' and Class Members' privacy. Plaintiffs bring this
4 action for legal and equitable remedies resulting from these illegal actions.

5 PARTIES

6 7. Plaintiff M.D. is a California citizen who resides in Whittier, California. On
7 December 6, 2022, and January 4, 2023, Plaintiff M.D. was prescribed and ordered Sildenafil
8 erectile dysfunction medication through the Website. Unbeknownst to Plaintiff M.D., Google and
9 Facebook intercepted protected health information ("PHI") related to his prescription medication
10 through their proprietary software codes, as described more thoroughly below. Due to the
11 surreptitious nature of the interceptions at issue, Plaintiff M.D. did not realize confidential
12 information related to his medical prescription was disclosed to third parties until September 2024.
13 Plaintiff M.D. was in California when he ordered prescription medication through the Website.

14 8. In addition to information related to his prescription medication, Defendants also
15 intercepted Plaintiff M.D.'s personally identifiable information ("PII"), including his first and last
16 name, email address, and date of birth. Subsequently, as a result of Defendants' conduct, Plaintiff
17 M.D. has received targeted advertisements relating to erectile dysfunction medications.

18 9. Plaintiff O.F. is a Pennsylvania citizen who resides in Philadelphia, Pennsylvania.
19 In January 2022, Plaintiff O.F. was prescribed and ordered Sildenafil erectile dysfunction
20 medication through the Website. Unbeknownst to Plaintiff O.F., Google and Facebook intercepted
21 PHI related to his prescription medication through their proprietary software codes, as described
22 more thoroughly below. Due to the surreptitious nature of the interceptions at issue, Plaintiff O.F.
23 did not realize confidential information related to his medical prescription was disclosed to third
24 parties until September 2024. Plaintiff O.F. was in Pennsylvania when he ordered prescription
25 medication through the Website.

26 10. In addition to information related to his prescription medication, Defendants also
27 intercepted Plaintiff O.F.'s PII, including his first and last name, email address, and date of birth.

1 Subsequently, as a result of Defendants' conduct, Plaintiff O.F. has received targeted
2 advertisements relating to erectile dysfunction medications.

3 11. Plaintiff J.P. is a Maryland citizen who resides in Silver Spring, Maryland. On or
4 around August 3, 2024, Plaintiff J.P. was prescribed and ordered Sildenafil erectile dysfunction
5 medication through the Website. Unbeknownst to Plaintiff J.P., Google and Facebook intercepted
6 PHI related to his prescription medication through their proprietary software codes, as described
7 more thoroughly below. Due to the surreptitious nature of the interceptions at issue, Plaintiff O.F.
8 did not realize confidential information related to his medical prescription was disclosed to third
9 parties until September 2024. Plaintiff O.F. was in Maryland when he ordered prescription
10 medication through the Website.

11 12. In addition to information related to his prescription medication, Defendants also
12 intercepted Plaintiff J.P.'s PII, including his first and last name, email address, and date of birth.
13 Subsequently, as a result of Defendants' conduct, Plaintiff J.P. has received targeted
14 advertisements relating to erectile dysfunction medications.

15 13. Facebook and Google committed the interceptions at issue without Plaintiffs'
16 knowledge, consent, or express written authorization. Such acts are egregious violations of
17 Plaintiffs' right to privacy.

18 14. Defendant Google LLC is a Delaware limited liability company with its principal
19 place of business located in Mountain View, California. At all times, Defendant Google knew that
20 the incorporation of its software onto the Website would result in its interception of PHI and other
21 sensitive data from the Website. Defendant Google, as the creator of its SDK, knew that it
22 intercepted each of a users' interactions on the Website that incorporated its technology.
23 Defendant Google has consistently come under scrutiny for incorporating its technology on
24 websites that involve the transmittal of sensitive data, including health information, but continues
25 to do so. Despite this, Google continued to encourage companies, like Blue Chew, to embed its
26 tracking technology on the Website, from which it intercepted BlueChew patients' sensitive health
27 data. Defendant Google intends to intercept this protected and sensitive health data due to the
28 value it holds for targeted advertising.

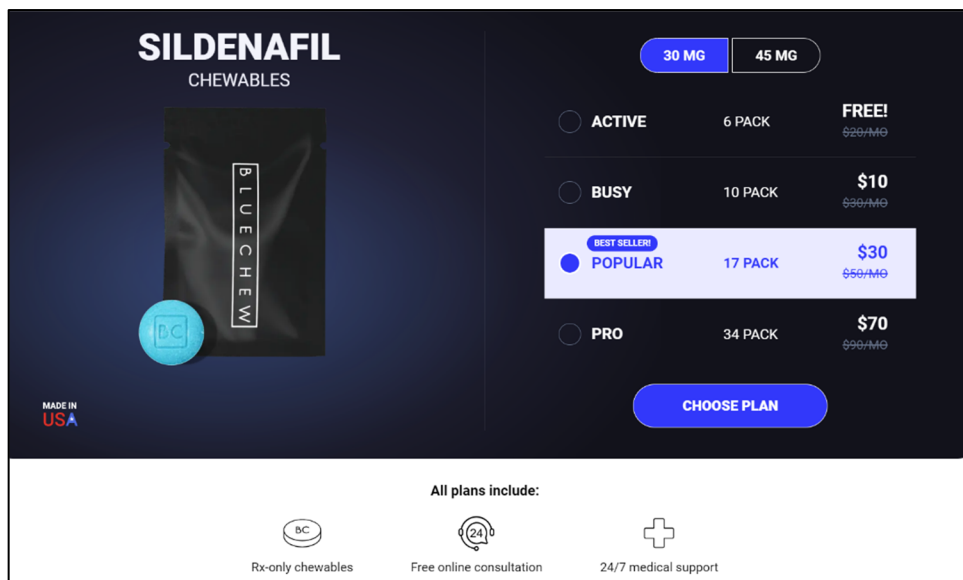
20. Consumers can only order prescription medication from BlueChew through its Website. When patients visit the Website, they are brought to BlueChew's homepage to order a prescription.

Figure 1:



21. Once a consumer clicks "GET STARTED," they are brought to an additional page to select a prescription plan.

Figure 2:



22. After selecting a prescription plan, patients are directed to complete a “medical profile” questionnaire, to determine whether they qualify for their selected prescription.

Figure 3:

MEDICAL PROFILE

Please answer the following questions to get your order approved.

1. Enter your personal information.

Legal First Name (as it appears on ID) [Text Input Field]

Legal Last Name (as it appears on ID) [Text Input Field]

Birth Date (MM/DD/YYYY) [Text Input Field]

23. When completing their medical profile on the Website, consumers are asked a range of health-related questions and asked to provide basic PII, including first and last name and date of birth.

24. If a patient is approved for their selected prescription medication, they are brought to a checkout page to complete their purchase.

Figure 4:

CHECKOUT

Shipping Address

Legal First Name* [Text Input Field] Legal Last Name* [Text Input Field]

First name is required Last name is required

Street Address* [Text Input Field] Apt, suite, etc. (Optional) [Text Input Field]

City* [Text Input Field]

State* [Dropdown Menu]

Zip Code* [Text Input Field]

Phone* [Text Input Field]

Add Shipping Address [Blue Button]

SILDENAFIL Chewables [Image of Product]

POPULAR 17 PACK | 30 MG (\$50/MO)

GET20 [Blue Button]

Coupon Applied!

Price:	\$50.00 /MO
Shipping:	TBD
Coupon:	-\$20.00
Handling Fee & Tax:	TBD
Grand Total:	\$30.00

25. At no point during the checkout process are patients alerted that information related to their prescription medication is being intercepted by third parties.

B. Facebook’s Tracking Technology on the BlueChew Website

26. Facebook describes itself as a “real identity platform,”³ meaning users are allowed only one account and must share “the name they go by in everyday life.”⁴ To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.⁵

27. In 2023, Facebook generated over \$134 billion in revenue.⁶ With respect to the apps offered by Facebook, substantially all of Facebook’s revenue is generated by selling advertising space.⁷

28. Facebook sells advertising space by highlighting its ability to target users.⁸ Facebook can target users effectively because it surveils user activity on and off its site.⁹ This allows Facebook to make inferences about users beyond what they explicitly disclose, like their “interests,” “behavior,” and “connections.”¹⁰ Facebook compiles this information into a generalized dataset called “Core Audiences,” which allows advertisers to reach precise audiences based on specified targeting types.¹¹

³ Sam Schechner & Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL ST. J. (Oct. 21, 2021, 4:05 PM), <https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701>.

⁴ FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

⁵ FACEBOOK, SIGN UP, <https://www.facebook.com>.

⁶ FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2023 RESULTS; INITIATES QUARTERLY DIVIDEND, https://s21.q4cdn.com/399680738/files/doc_news/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend-2024.pdf at 8.

⁷ *Id.*

⁸ FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, <https://www.facebook.com/business/help/205029060038706>.

⁹ FACEBOOK, ABOUT META PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

¹⁰ FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting>.

¹¹ FACEBOOK, <https://www.facebook.com/business/news/Core-Audiences>.

29. Advertisers can also build “Custom Audiences.”¹² Custom Audiences enables advertisers to reach “people who have already shown interest in [their] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.”¹³ With Custom Audiences, advertisers can target existing customers directly and build “Lookalike Audiences,” which “leverage[] information such as demographics, interests and behaviors from your source audience to find new people who share similar qualities.”¹⁴ Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: (1) by manually uploading contact information for customers or (2) by utilizing Facebook’s “Business Tools.”¹⁵

30. As Facebook puts it, the Business Tools “help website owners and publishers, app developers, and business partners, including advertisers and others, integrate with [Facebook], understand and measure their products and services, and better reach and serve people who might be interested in their products and services.”¹⁶ Put more succinctly, Facebook’s Business Tools are bits of code that advertisers can integrate into their websites, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

31. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage’s Universal Resource Locator (“URL”) and metadata, or when a user downloads a mobile application or makes a purchase.¹⁷ Facebook’s Business Tools can also

¹² FACEBOOK, ABOUT CUSTOM AUDIENCES, <https://www.facebook.com/business/help/744354708981227?id=2469097953376494>.

¹³ FACEBOOK, AUDIENCE AD TARGETING, <https://www.facebook.com/business/ads/ad-targeting>.

¹⁴ FACEBOOK, ABOUT LOOKALIKE AUDIENCES, <https://www.facebook.com/business/help/164749007013531?id=401668390442328>.

¹⁵ FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494>.

¹⁶ FACEBOOK, THE META BUSINESS TOOLS, <https://www.facebook.com/help/331509497253087>.

¹⁷ See FACEBOOK, META FOR DEVELOPERS: META PIXEL, ADVANCED, <https://developers.facebook.com/docs/meta-pixel/advanced/>; see also FACEBOOK, BEST PRACTICES FOR META PIXEL SETUP, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>; FACEBOOK, META FOR DEVELOPERS: MARKETING API - APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/>.

1 track other events. Facebook offers a menu of “standard events” from which advertisers can
 2 choose, including what content a visitor views or purchases.¹⁸ Advertisers can even create their
 3 own tracking parameters by building a “custom event.”¹⁹

4 32. One such Business Tool is the Facebook Tracking Pixel. Facebook offers this piece
 5 of code to advertisers, like BlueChew, to integrate into their website. As the name implies, the
 6 Facebook Tracking Pixel “tracks the people and type of actions they take.”²⁰ When a user accesses
 7 a website hosting the Facebook Tracking Pixel, Facebook’s software script surreptitiously directs
 8 the user’s browser to contemporaneously send a separate message to Facebook’s servers. This
 9 second secret and contemporaneous transmission contains the original GET request sent to the host
 10 website, along with additional data that the Facebook Tracking Pixel is configured to collect. This
 11 transmission is initiated by Facebook code and concurrent with the communications with the host
 12 website. At relevant times, two sets of code were thus automatically run as part of the browser’s
 13 attempt to load and read BlueChew’s Website—BlueChew’s own code and Facebook’s embedded
 14 code.

15 33. Facebook’s own documentation makes clear how extensively the Facebook
 16 Tracking Pixel tracks private information. It describes the Facebook Tracking Pixel as code that
 17 Facebook’s business customers can put on their website to “[m]ake sure your ads are shown to the
 18 right people[] [and] *find . . . people who have visited a specific page or taken a desired action on*
 19 *your website*” (emphasis added).²¹

20 34. Facebook instructs such business customers that:

21 Once you’ve set up the [Facebook Tracking] Pixel, *the pixel will log when someone*
 22 *takes an action on your website*. Examples of actions include adding an item to their
 shopping cart or making a purchase. *The Pixel receives these actions, or events,*

23 ¹⁸ FACEBOOK, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS,
 24 <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>.

25 ¹⁹ FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,
 26 <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; *see also*
 FACEBOOK, META FOR DEVELOPERS: MARKETING API – APP EVENTS API,
<https://developers.facebook.com/docs/marketing-api/app-event-api/>.

27 ²⁰ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting>.

28 ²¹ META, ABOUT META PIXEL,
<https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

which you can view on your [Facebook Tracking] Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. ***You'll also have options to reach those customers again through future Meta ads.***²²

35. This tracked information includes private data revealing prescribed medications purchased by patients on the BlueChew Website.

36. The Facebook Tracking Pixel code enables Facebook not only to help BlueChew with advertising to its own patients outside the Website, but also includes individual patients among groups targeted by ***other*** Facebook advertisers relating to the conditions about which patients communicated on BlueChew's Website.

37. Facebook's Business Help Center explains:

Meta ***uses event data to show ads to people who are likely to be interested in them.*** One type of marketing data is website events, which are ***actions that people take on your website.***²³

38. In other words, Facebook sells advertising space by highlighting its ability to target users.²⁴ Facebook can target users so effectively because it surveils user activity both on and off its site.²⁵ This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behaviors," and connections.²⁶

39. An example illustrates how the Facebook Tracking Pixel works. Take an individual who, at relevant times, navigated to BlueChew's Website and clicked on a link to purchase prescription medication. When that link was clicked, the individual's browser sent a GET request to BlueChew's server requesting the server to load the particular webpage. Then, the Facebook Tracking Pixel, Facebook's embedded code, written in JavaScript, sent secret instructions back to the individual's browser, without alerting the individual that this was happening. Facebook caused

²² *Id.* (emphasis added).

²³ META, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142> (emphasis added).

²⁴ META, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, <https://www.facebook.com/business/help/205029060038706> (last visited May 21, 2024).

²⁵ META, ABOUT META PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

²⁶ META, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting>.

the browser to secretly duplicate the communication with BlueChew, transmitting it to Facebook's servers, alongside additional information that transcribed the communication's content and the individual's identity.

40. Examples of these interceptions from the BlueChew Website are provided in Figures 5 and 6 below:

Figures 5 and 6:

```

id      3074830112604017
ev      CompleteRegistration
dl      https://app.bluechew.com/medical
rl
if      false
ts      1725047922452
cd[fn]  Jimmy
cd[in]   Anderson
cd[db]   July 10, 2001
cd[st]   Florida
cd[em]   thommy5431@yahoo.com
sw      3072
sh      1728
udff[em] 2a9a22d88b031064ea86ff104d1cabf6b14a866c2a4adf136def1330b49fecbb
v       2.9.166
r       stable
ec      7
o       6174
fbp     fb.1.1725047569640.118057358755152954
ler     empty
cdl     API_unavailable
it      1725047569594
coo     false
eid     2dbef376-e9f9-4d60-aa6f-57e6cc7f8680
rqm     GET
  
```

id	3074830112604017
ev	AddToCart
dl	https://app.bluechew.com/plans
rl	
if	false
ts	1725047590601
cd[content_id]	1
sw	3072
sh	1728
v	2.9.166
r	stable
ec	1
o	4126
fbp	fb.1.1725047569640.118057358755152954
ler	empty
cdl	API_unavailable
it	1725047569594
coo	false
eid	4e93e818-65da-46db-8289-afa239434f77
rgm	GET

41. Through the Facebook Tracking Pixel, Defendant Facebook intercepted and recorded “AddToCart” and “CompleteRegistration” events, which detail information about which prescription the patient was purchasing on the Website.

42. As shown in Figure 5, Facebook intercepts patients’ PII, including first and last name, date of birth, and email address when they are completing the BlueChew medical profile.

43. As shown in Figure 6, Facebook intercepts information related to patients’ prescription medications.

44. Each of BlueChew’s medications are assigned their own unique content ID. These unique IDs indicate the type of medication being purchased by patients, as well as the quantity and dosage. For example, the content ID “1” indicates that a patient has selected a 6-pack of BlueChew’s 30 mg Sildenafil prescription medication. Similar unique IDs are used for all varieties of BlueChew’s prescriptions. Based on these unique IDs, Facebook possesses information about the prescription medication being purchased by BlueChew’s patients.

1 45. Each time Facebook intercepted this activity data through the Facebook Tracking
2 Pixel, it also disclosed a patient's personally identifiable information, including their Facebook ID
3 ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it,
4 any ordinary person can look up the user's Facebook profile and name. Notably, while Facebook
5 can easily identify any individual on its Facebook platform with only their unique FID, so too can
6 any ordinary person who comes into possession of an FID. Facebook admits as much on its
7 website. Indeed, ordinary persons who come into possession of the FID can connect to any
8 Facebook profile.

9 46. A user who accessed the Website while logged into Facebook transmitted what is
10 known as a "c_user cookie" to Facebook, which contains that user's unencrypted FID.

11 47. When a visitor's browser had recently logged out of an account, Facebook
12 compelled the visitor's browser to send a smaller set of cookies.

13 48. One such cookie was the "fr cookie" which contained, at least, an encrypted FID
14 and browser identifier.²⁷ Facebook, at a minimum, used the fr cookie to identify users.²⁸

15 49. If a visitor had never created an account, an even smaller set of cookies was
16 transmitted.

17 50. At each stage, the Website also utilized the "_fbp cookie," which attached to a
18 browser as a first-party cookie, and which Facebook used to identify a browser and a user.²⁹

19 51. The c_user cookie expires after 90 days if the user checked the "keep me logged in"
20 checkbox on the website.³⁰ Otherwise, the c_user cookie is cleared when the browser exits.³¹

21 52. The fr cookie expires after 90 days unless the visitor's browser logs back into
22

23
24 ²⁷ DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21,
2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.

25 ²⁸ FACEBOOK, PRIVACY CENTER – COOKIES POLICY,
<https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3>.

26 ²⁹ *Id.*

27 ³⁰ Seralthan, FACEBOOK COOKIES ANALYSIS (Mar. 14, 2019),
<https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbf8a>.

28 ³¹ *Id.*

Facebook.³² If that happens, the time resets, and another 90 days begins to accrue.³³

53. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.³⁴ If that happens, the time resets, and another 90 days begins to accrue.³⁵

54. The Facebook Tracking Pixel used both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—*i.e.*, the Website.³⁶ A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—*i.e.*, Facebook.³⁷ The _fbp cookie was always transmitted as a first-party cookie. A duplicate _fbp cookie was sometimes sent as a third-party cookie, depending on whether the browser had recently logged into Facebook.

55. Facebook, at a minimum, used the fr, _fbp, and c_user cookies to link to FIDs and corresponding Facebook profiles. Facebook intercepted these identifiers alongside the event data.

56. Alternatively, Facebook can also match this prescription information to the specific BlueChew patient based on the PII intercepted from the patient's medical profile.

57. After collecting and intercepting the information described in the preceding paragraphs, Facebook processed, analyzed, and assimilated it into datasets like Core Audiences and Custom Audiences.

58. Plaintiffs never consented, agreed, authorized, or otherwise permitted Facebook to disclose his PII and PHI.

C. Google's Tracking Technology on the BlueChew Website

59. Google is one of the most valuable publicly traded companies in the world with a market capitalization of over \$1 trillion dollars. Google fancies itself a "tech" company, but

³² *See id.*

³³ Confirmable through developer tools.

³⁴ FACEBOOK, PRIVACY CENTER – COOKIES POLICY, <https://mbasic.facebook.com/privacy/policies/cookies/printable/#annotation-1>.

³⁵ Also confirmable through developer tools.

³⁶ PC MAG, FIRST-PARTY COOKIE, <https://www.pcmag.com/encyclopedia/term/first-party-cookie>. This is confirmable by using developer tools to inspect a website's cookies and track network activity.

³⁷ PC MAG, THIRD-PARTY COOKIE, <https://www.pcmag.com/encyclopedia/term/third-party-cookie>. This is also confirmable by tracking network activity.

Google, at its core, is an advertising company.

60. Google “make[s] money” from “advertising products [that] deliver relevant ads at just the right time,” generating “revenues primarily by delivering both performance advertising and brand advertising.”³⁸ In 2020, Google generated \$146.9 billion in advertising revenue, which amounted to more than 80 percent of Google’s total revenues for the year. Google generated an even higher percentage of its total revenues from advertising in prior years:

Figure 7:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	\$257.6 billion	\$209.5	81.33%
2020	\$182.5 billion	\$146.9 billion	80.49%
2019	\$161.9 billion	\$134.8 billion	83.29%
2018	\$136.8 billion	\$116.5 billion	85.12%

61. Google offers several analytics products, including SDKs and a tracking pixel, which exist solely to help drive ad revenue. For instance, Google’s SDK and pixel integrate with Google’s advertising offerings, such as Google Ads, Search Ads 360, Google Cloud, and Google Ad Manager, to direct more individuals to use Google’s ad network and products increasing Google’s overall ad revenue. Products like Google’s SDK and its tracking pixel also improve the company’s advertising network and capabilities by providing more wholesome profiles and data points on individuals.

62. One of these SDKs and tracking pixels is Google Analytics. Google first launched a version of Google Analytics in 2005 as a tool for website traffic analysis. In 2007, Google launched Google Analytics Synchronous code with new tracking functionality, such as the ability to track commerce transactions. Two years later, Google launched the Google Analytics Asynchronous code, which allowed webpages to load faster and improved data collection and accuracy.

63. Google continued updating its analytics platform, launching Universal Analytics in 2012. Universal Analytics offered new tracking codes and tools that provided more in-depth

³⁸ ALPHABET INC., ANNUAL REPORT (FORM 10-K) (Feb. 2, 2021), available at <https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm>.

1 information about user behavior. Also, Universal Analytics enabled tracking the same user across
2 multiple devices through its addition of the User-ID feature, which “associate[s] a persistent ID for
3 a single user with that user’s engagement data from one or more sessions initiated from one or
4 more devices.”

5 64. In 2020, Google launched Google Analytics 4, a platform combining Google
6 Analytics with Firebase to analyze both app and web activity.

7 65. Since launching Google Analytics, Google has become one of the most popular web
8 analytics platforms on the internet. Indeed, Google had a \$62.6 billion increase in advertising
9 revenues in 2021, compared to 2020, after launching its most recent version of Google Analytics.

10 66. Google touts Google Analytics as a marketing platform that offers “a complete
11 understanding of your customers across devices and platforms.”³⁹ It allows companies and
12 advertisers that utilize it to “understand how your customers interact across your sites and apps,
13 throughout their entire lifestyle,” “uncover new insights and anticipate future customer actions with
14 Google’s machine learning to get more value out of your data,” “take action to optimize marketing
15 performance with integrations across Google’s advertising and publisher tools,” and “quickly
16 analyze your data and collaborate with an easy-to-use interface and shareable reports.”⁴⁰

17 67. Google Analytics is incorporated into third-party websites and apps, including the
18 Website, by adding a small piece of JavaScript measurement code to each page on the site. This
19 code immediately intercepts a user’s interaction with the webpage every time the user visits it,
20 including what pages they visit and what they click on. The code also collects PII, as shown in
21 Figures 8 and 9 below.

22
23
24
25
26
27 ³⁹ *Analytics*, GOOGLE, <https://marketingplatform.google.com/about/analytics/> (last visited Jan. 10, 2023).

28 ⁴⁰ *Id.*

Figures 8 and 9:

```

sid      1725047568
sct      1
seg      1
dl       https://app.bluechew.com/medical
dr       https://app.bluechew.com/register
dt       Medical | BlueChew®
en       CompleteRegistration
_c       1
_ee      1
ep.first_name Jimmy
ep.last_name Anderson
ep.state  Florida
ep.email  thommy5431@yahoo.com
ep.dob    July 10, 2001
ep.event_id 2dbef376-e9f9-4d60-aa6f-57e6cc7f8680
ep.click_id
ep.uuid_c1

```

```

sid      1725047568
sct      1
seg      1
dl       https://app.bluechew.com/plans
dt       BlueChew® Plans | Choose Sildenafil, Tadalafil, or Vardenafil
en       add_to_cart
_ee      1
pr1      id1
epn.product_id 1
ep.event_id 4e93e818-65da-46db-8289-afa239434f77
ep.click_id
ep.uuid_c1

```

68. As shown in Figure 8, Google is intercepting patients' PII, including first and last name, date of birth, and email address when they are completing the BlueChew medical profile.

69. As shown in Figure 9, Google is intercepting information related to patients' prescription medications.

70. As discussed, *supra*, each of BlueChew's medications are provided their own unique product ID. These unique IDs will indicate not only the type of medication being

1 purchased by patients, but also the quantity and dosage. The product ID “1” indicates that a patient
2 has selected a 6-pack of BlueChew’s 30 mg Sildenafil prescription medication.

3 71. Once Google’s software code collects the data, it packages the information and
4 sends it to Google Analytics for processing. Google Analytics enables the company or advertiser
5 to customize the processing of the data, such as applying filters. Once the data is processed, it is
6 stored on a Google Analytics database and cannot be changed.

7 72. After the data has been processed and stored in the database, Google uses this data
8 to generate reports to help analyze the data from the webpages. These include reports on
9 acquisition (e.g., information about where your traffic originates, the methods by which users
10 arrive at your site or app, and the marketing efforts you use to drive traffic), engagement (e.g.,
11 measure user engagement by the events and conversion events that users trigger and the web pages
12 and app screens that user visits, and demographics (e.g., classify your users by age, location,
13 language, and gender, along with interests they express through their online browsing and purchase
14 activities).

15 73. In addition to using the data collected through Google Analytics to provide
16 marketing and analytics services, Google also uses the data collected through Google Analytics to
17 improve its ad targeting capabilities and data points on users.

18 74. Google Analytics links with Google Ads, allowing the data intercepted by Google
19 Analytics to be utilized for targeted advertising purposes.⁴¹ Such practices were in effect on the
20 BlueChew Website for targeted advertising purposes.

21 75. The Website utilizes Google’s pixel and SDK. As a result, Google intercepted
22 patients’ interactions on the Website, including their PII and PHI. Google received at least
23 “Custom Events” and URLs that disclosed the name of the prescription medication and the
24 medication quantity and dosage. Google also received additional PII, including first and last name,
25 email address, and date of birth, that uniquely identify the patient, as shown below in Figures 8 and
26 9.

27
28 ⁴¹ <https://support.google.com/analytics/answer/9379420?hl=en#zippy=%2Cin-this-article>

76. Plaintiffs and Class Members provided their PII, PHI, and other sensitive data to BlueChew to obtain medical prescriptions. This information was intercepted by Google without Plaintiffs' consent or knowledge.

77. By law, Plaintiffs are entitled to privacy in their protected health information and confidential communications. Defendants deprived Plaintiffs of their privacy rights when they: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiffs' and other online patients' confidential communications, personally identifiable information, and protected health information; (2) disclosed and/or intercepted patients' protected health information; and (3) undertook this pattern of conduct without notifying Plaintiffs and without obtaining their express written consent.

CLASS ACTION ALLEGATIONS

78. Plaintiff M.D. brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of a class defined as all natural persons in California who, during the class period, purchased medication on www.bluechew.com (the "California Class").

79. Plaintiff O.F. brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of a class defined as all natural persons in Pennsylvania who, during the class period, purchased medication on www.bluechew.com (the "Pennsylvania Class").

80. Plaintiff J.P. brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of a class defined as all natural persons in Maryland who, during the class period, purchased medication on www.bluechew.com (the "Maryland Class").

81. Plaintiffs reserve the right to modify the class definitions or add sub-classes as necessary prior to filing a motion for class certification.

82. The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgement.

83. Excluded from the Classes are Defendants; any affiliate, parent, or subsidiary of Defendants; any entity in which Defendants have a controlling interest; any officer, director, or employee of Defendants; any successor or assign of Defendants; anyone employed by counsel in

1 this action; any judge to whom this case is assigned, his/her spouse and immediate family
2 members; and members of the judge's staff.

3 84. Numerosity. Members of the Classes are so numerous that joinder of all members is
4 impracticable. The exact number of Class Members is unknown to Plaintiffs at this time. However,
5 it is estimated that there are at least thousands of individuals in the Classes. The identity of such
6 membership is readily ascertainable from Defendants' records.

7 85. Typicality. Plaintiffs' claims are typical of the claims of the Classes because
8 Plaintiffs used www.bluechew.com to purchase a prescription for erectile dysfunction medication
9 and had their personally identifiable information and protected health information disclosed to
10 Facebook and Google without their express written authorization or knowledge. Plaintiffs' claims
11 are based on the same legal theories as the claims of other Class Members.

12 86. Adequacy. Plaintiffs are prepared to take all necessary steps to represent fairly and
13 adequately the interests of the Class Members. Plaintiffs' interests are coincident with, and not
14 antagonistic to, those of the members of the Classes. Plaintiffs are represented by attorneys with
15 experience in the prosecution of class action litigation, generally, and in the emerging field of
16 digital privacy litigation, specifically. Plaintiffs' attorneys are committed to vigorously
17 prosecuting this action on behalf of the members of the Classes.

18 87. Superiority. Class action treatment is the superior method for the fair and efficient
19 adjudication of this controversy. Such treatment permits a large number of similarly situated
20 persons to prosecute their common claims in a single forum simultaneously, efficiently, and
21 without the unnecessary duplication of evidence, effort, or expense that numerous individual
22 actions would engender. The benefits of proceeding through the class mechanism, including
23 providing injured persons or entities a method for obtaining redress on claims that could not
24 practicably be pursued individually, substantially outweigh any potential difficulties in the
25 management of this class action. Plaintiffs know of no special difficulty to be encountered in
26 litigating this action that would preclude its maintenance as a class action.

27 88. Commonality. Questions of law and fact common to the members of the Classes
28 predominate over questions that may affect only individual members of the Classes because

Defendants have acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendants' wrongful conduct. Questions of law and fact common to the Classes include:

- a. Whether Defendants intentionally tapped the lines of internet communication between patients and their healthcare provider;
- b. Whether Defendants' software code surreptitiously recorded personally identifiable information, protected health information, and related communications;
- c. Whether Facebook and Google are third-party eavesdroppers;
- d. Whether Defendants' disclosures of personally identifiable information, protected health information, and related communications constituted an affirmative act of communication;
- e. Whether Defendants violated Plaintiffs' and Class Members' privacy rights by using their software code to record and communicate patients' confidential medical communications;
- f. Whether Plaintiffs and Class Members are entitled to damages under CIPA, WESCA, MWESCA, or any other relevant statute; and
- g. Whether Defendants' actions violated Plaintiffs' and Class Members' privacy rights as provided by the California Constitution.

COUNT I

Violation of the California Invasion of Privacy Act, Cal. Penal Code § 631

89. Plaintiff M.D. repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the California Class against Defendants.

90. The California Invasion of Privacy Act (the "CIPA") is codified at California Penal Code Sections 630 to 638. The CIPA begins with its statement of purpose—namely, that the purpose of the CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices

1 and techniques for the purpose of eavesdropping upon private communications . . .” Cal. Penal
2 Code § 630.

3 91. A person violates California Penal Code Section 631(a), if:

4 by means of any machine, instrument, or contrivance, or in any other manner, [s/he]
5 intentionally taps, or makes any unauthorized connection, whether physically,
6 electrically, acoustically, inductively, or otherwise, with any telegraph or telephone
7 wire, line, cable, or instrument, including the wire, line, cable, or instrument of any
8 internal telephonic communication system, or [s/he] willfully and without the consent
9 of all parties to the communication, or in any unauthorized manner, reads, or attempts
10 to read, or to learn the contents or meaning of any message, report, or communication
while the same is in transit or passing over any wire, line, or cable, or is being sent
from, or received at any place within this state; or [s/he] uses, or attempts to use, in
any manner, or for any purpose, or to communicate in any way, any information so
obtained . . .⁴²

11 92. To avoid liability under section 631(a), a defendant must show it had the consent of
12 all parties to a communication.

13 93. At all relevant times, Defendants tracked and intercepted Plaintiff M.D.’s and Class
14 Members’ internet communications while using www.bluechew.com to buy prescription
15 medications. These communications were intercepted without the authorization and consent of
16 Plaintiff M.D. and members of the California Class.

17 94. Defendants intended to learn some meaning of the content in the URLs and the
18 content the visitors requested.

19 95. The following items constitute “machine[s], instrument[s], or contrivance[s]” under
20 the CIPA, and even if they do not, Defendants’ SDKs and other software code fall under the broad
21 catch-all category of “any other manner”:

- 22 a. The computer codes and programs Facebook and Google used to track Plaintiff
- 23 M.D. and California Class Members’ communications while they were navigating
- 24 www.bluechew.com;
- 25 b. Plaintiff M.D.’s and California Class Members’ browsers;
- 26 c. Plaintiff M.D.’s and California Class Members’ computing and mobile devices;

27
28 ⁴² Cal. Penal Code § 631(a).

- d. Defendants' web and ad servers;
- e. The web and ad servers from which Facebook and Google tracked and intercepted Plaintiff M.D.'s and California Class Members' communications while they were using a web browser to access or navigate www.bluechew.com;
- f. The computer codes and programs used by Facebook and Google to effectuate their tracking and interception of Plaintiff M.D.'s and California Class Members' communications while they were using a browser to visit www.bluechew.com; and
- g. The plan Defendants' carried out to effectuate its tracking and interception of Plaintiff M.D.'s and California Class Members' communications while they were using a web browser or mobile device to visit www.bluechew.com.

96. At all relevant times, Defendants, through their SDKs and other software code, intentionally tapped or made unauthorized connections with, the lines of internet communications between Plaintiff M.D. and California Class Members and the Website without the consent of all parties to the communication.

97. Defendants, willfully and without the consent of Plaintiff M.D. and California Class Members, read or attempted to read, or learn the contents or meaning of Plaintiff M.D.'s and California Class Members' communications to BlueChew while the communications are in transit or passing over any wire, line or cable, or were being received at any place within California when it intercepted Plaintiff M.D.'s and California Class Members' communications and data with BlueChew.

98. Defendants used or attempted to use the communications and information they received through their tracking technology, including to supply advertising services.

99. The information intercepted by Defendants, such as information related to prescription medications, constituted protected health information.

100. As a result of the above violations, Defendants are liable to Plaintiff M.D. and other California Class Members in the amount of \$5,000 dollars per violation or three times the amount of actual damages, whichever is greater. Additionally, California Penal Code Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that

1 the plaintiff has suffered, or be threatened with, actual damages.”

2 101. Under the CIPA, Defendants are also liable for reasonable attorney’s fees, and other
3 litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be
4 determined by a jury, but sufficient to prevent the same or similar conduct by Defendants in the
5 future.

6 **COUNT II**
7 **Violation of the California Invasion of Privacy Act,**
8 **Cal. Penal Code § 632**

9 102. Plaintiff M.D. repeats the allegations contained in the paragraphs above as if fully
10 set forth herein and brings this count individually and on behalf of the members of the California
11 Class against Defendants.

12 103. Cal. Penal Code § 632 prohibits “intentionally and without the consent of all parties
13 to a confidential communication,” the “use[] [of] an electronic amplifying or recording device to
14 eavesdrop upon or record the confidential communication.”

15 104. Section 632 defines “confidential communication” as “any communication carried
16 on in circumstances as may reasonably indicate that any party to the communication desires it to be
17 confined to the parties thereto[.]”

18 105. Plaintiff M.D.’s and California Class Members’ communications to BlueChew,
19 including their sensitive personal and health information, such as information related to their
20 prescription medications, were confidential communications for purposes of § 632, because
21 Plaintiff M.D. and California Class Members had an objectively reasonable expectation of privacy
22 in this data.

23 106. Plaintiff M.D. and California Class Members expected their communications to
24 BlueChew to be confined to BlueChew due to the confidential nature of those communications.
25 Plaintiff M.D. and California Class Members did not expect third parties, specifically Facebook or
26 Google, to secretly eavesdrop upon or record this information and their communications.

27 107. Facebook’s and Google’s tracking technology are electronic amplifying or
28 recording devices for purposes of § 632.

108. By contemporaneously intercepting and recording Plaintiff M.D.’s and California

1 Class Members' confidential communications to BlueChew through this technology, Defendants
2 eavesdropped and/or recorded confidential communications through an electronic amplifying or
3 recording device in violation of § 632 of CIPA.

4 109. At no time did Plaintiff M.D. or California Class Members consent to Defendants'
5 conduct, nor could they reasonably expect that their communications to BlueChew would be
6 overheard or recorded by Defendants.

7 110. Defendants utilized Plaintiff M.D.'s and California Class Members' sensitive
8 personal and health information for their own purposes, including for targeted advertising.

9 111. Plaintiff M.D. and California Class Members seek statutory damages in accordance
10 with § 637.2(a) which provides for the greater of: (1) \$5,000 per violation; or (2) three times the
11 amount of damages sustained by Plaintiff M.D. and the California Class in an amount to be proven
12 at trial, as well as injunctive or other equitable relief.

13 112. Plaintiff M.D. and California Class Members have also suffered irreparable injury
14 from these unauthorized acts. Plaintiff M.D.'s and California Class Members' sensitive data has
15 been collected, viewed, accessed, stored, by Defendants, have not been destroyed, and due to the
16 continuing threat of such injury, have no adequate remedy at law. Plaintiff M.D. and California
17 Class Members are accordingly entitled to injunctive relief.

18 **COUNT III**

19 **Invasion of Privacy Under California's Constitution**

20 113. Plaintiff M.D. repeats the allegations contained in the paragraphs above as if fully
21 set forth herein and brings this count individually and on behalf of the members of the California
22 Class against Defendants.

23 114. Plaintiff M.D. and California Class Members have an interest in: (1) precluding the
24 dissemination and/or misuse of their sensitive, confidential communications and protected health
25 information; and (2) making personal decisions and/or conducting personal activities without
26 observation, intrusion, or interference, including, but not limited to, the right to visit and interact
27 with various internet sites without being subjected to wiretaps without Plaintiff M.D.'s and
28 California Class Members' knowledge or consent.

115. At all relevant times, by using the SDKs and other software codes to record and communicate patients' personal identifiers alongside their confidential medical communications, Defendants intentionally invaded Plaintiff M.D.'s and California Class Members' privacy rights under the California Constitution.

116. Plaintiff M.D. and California Class Members had a reasonable expectation that their communications, identities, health information, and other data would remain confidential, and that Defendants would not install wiretaps on www.bluechew.com.

117. Plaintiff M.D. and California Class Members did not authorize Defendants to record and transmit Plaintiff M.D.'s and California Class Members' private medical communications alongside their personally identifiable and health information.

118. This invasion of privacy was serious in nature, scope, and impact because it related to patients' private medical communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

119. Accordingly, Plaintiff M.D. and California Class Members seek all relief available for invasion of privacy under the California Constitution.

COUNT IV
**Violation of the Pennsylvania Wiretapping Act,
 18 Pa. Cons. Stat. § 5701**

120. Plaintiff O.F. repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Pennsylvania Class against Defendants.

121. The Pennsylvania Wiretapping Act prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

122. Any person who intercepts, discloses, or uses or procures any other person to

1 intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is
 2 subject to a civil action for (1) actual damages, not less than liquidated damages computed at a rate
 3 of \$100 per day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3)
 4 reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

5 123. "Intercept" is defined as the "[a]ural or other acquisition of the contents of any wire,
 6 electronic or oral communication through the use of any electronic, mechanical or other device."
 7 18 Pa. Cons. Stat. § 5702. "Electronic, mechanical or other device," in turn, means "[a]ny device
 8 or apparatus ... that can be used to intercept a wire, electronic or oral communication[.]" *Id.*

9 124. The following constitutes a device within the meaning of 18 Pa. Cons. Stat. § 5702:

- 10 a. The computer codes and programs that Defendant used to track Plaintiff O.F. and
- 11 Pennsylvania Class Members' communications while navigating the website;
- 12 b. Plaintiff O.F.'s and Pennsylvania Class Members' web browsers;
- 13 c. Plaintiff O.F.'s and Pennsylvania Class Members' computing devices;
- 14 d. Defendants' web servers;
- 15 e. The web servers from which Facebook and Google received the Plaintiff O.F.'s and
- 16 Pennsylvania Class Members' communications while they were using a web
- 17 browser to access the Website; and
- 18 f. The plan Defendants carried out to effectuate their tracking of Plaintiff O.F.'s and
- 19 Pennsylvania Class Members' communications while using a web browser to access
- 20 the website.

21 125. At all relevant times, Defendants intended to track and intercept Plaintiff O.F.'s and
 22 other Pennsylvania Class Members' internet communications while navigating the Website.
 23 Defendants intercepted these communications without authorization or consent from Plaintiff O.F.
 24 or Pennsylvania Class Members.

25 126. Defendants intended to learn the meaning of the content the patient requested while
 26 on the Website.

27 127. Plaintiff O.F. and Pennsylvania Class Members had a justified expectation under the
 28 circumstances that their electronic communications would not be intercepted.

128. Plaintiff O.F. and Pennsylvania Class Members were not aware that their electronic communications were being intercepted by Facebook and Google.

COUNT V

Violation of the Maryland Wiretapping and Electronic Surveillance Act Md. Code, Cts. & Jud. Proc. Code Sec. 10-401, et seq (Maryland Class)

129. Plaintiff J.P. repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Maryland Class against Defendants.

130. Maryland's Wiretapping and Electronic Surveillance Act ("MWESA") makes it unlawful to: (1) willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (2) willfully disclose, or endeavor to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subtitle; or (3) willfully use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication." Md. Cts. & Jud. Proc. Code Sec. 10-402.

131. Under the MWESA, "willfully" is defined as "an intentional violation or a reckless disregard of a known legal duty." *Benford v. Am. Broadcasting Co.*, 649 F. Supp. 9, 10 (D. Md. 1986).

132. "Electronic Communication" is defined as "[a]ny transfer of signals, writings, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." Md. Code. Cts. & Jud. Proc. Sec. 10-401(5)(i).

133. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Md. Code Cts. & Jud. Proc. Sec. 10-401(4).

134. “Contents” is defined as “any information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication.” Md. Code Cts. & Jud. Proc. Sec. 10-401(7).

135. As alleged above Facebook and Google intercepted Plaintiff J.P.’s and Maryland Subclass members’ electronic communications, including information that contained PHI and PII.

136. Plaintiff J.P.’s and Maryland Subclass members’ electronic communications were intercepted in Maryland.

137. At all relevant times, Defendants intended to intercept Plaintiff J.P.’s and Maryland Subclass members’ communications with www.bluechew.com. Plaintiff J.P. and Maryland Subclass members did not consent to such interceptions.

138. Defendants sought to profit and in fact did profit off the interception of Plaintiff J.P.’s and the Maryland Subclass members’ electronic communications while intentionally or recklessly disregarding its own legal duty.

139. The interception of Plaintiff J.P.’s and Maryland Subclass members PII and PHI constitutes an invasion of privacy sufficient to confer Article III standing.

140. Plaintiff J.P. and Maryland Subclass members seek all relief available under Md. Code Cts. & Jud. Proc. Secs. 10-410(a)(1)-(3), including statutory damages of \$100 per day for each day of violation or \$1,000, whichever is higher, punitive damages, and reasonable attorneys’ fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for relief and judgment, as follows:

- a. For a determination that this action is a proper class action;
- b. For an order certifying the Classes, naming Plaintiffs as representative of the Classes, and naming Plaintiffs’ attorneys as Class Counsel to represent the Classes;
- c. For an order declaring that Defendants’ conduct violated the statutes referenced herein;
- d. For an order finding in favor of Plaintiffs and the Classes on all counts

1 asserted herein;

- 2 e. For an award of compensatory damages, including statutory damages where
3 available, to Plaintiffs and the Class Members against Defendants for all
4 damages sustained as a result of Defendants' wrongdoing, in an amount to
5 be proven at trial;
- 6 f. For punitive damages, as warranted, in an amount to be determined at trial;
- 7 g. For an order requiring Defendants to disgorge revenues and profits
8 wrongfully obtained;
- 9 h. For prejudgment interest on all amounts awarded;
- 10 i. For injunctive relief as pleaded or as the Court may deem proper;
- 11 j. For an order awarding Plaintiffs and the Classes their reasonable attorneys'
12 fees and expenses and costs of suit; and
- 13 k. For an order granting Plaintiffs and Class Members such further relief as the
14 Court deems appropriate.

15 **DEMAND FOR JURY TRIAL**

16 Plaintiffs, on behalf of themselves and the proposed Classes, demand a trial by jury for all
17 of the claims asserted in this Complaint so triable.
18

19 Dated: January 6, 2025

Respectfully submitted,

20 **BURSOR & FISHER, P.A.**

21
22 By: /s/ L. Timothy Fisher
23 L. Timothy Fisher

24 L. Timothy Fisher (State Bar No. 191626)
25 1990 North California Blvd., 9th Floor
26 Walnut Creek, CA 94596
27 Telephone: (925) 300-4455
28 Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

Counsel for Plaintiffs